Cassandra Crossing/ Il crittografo e il Grande Fratello

(366)—David Chaum è padre di invenzioni rivoluzionarie nell'ambito della crittografia: teorizza la moneta digitale e il principio delle…

Cassandra Crossing/ Il crittografo e il Grande Fratello

Figure 1:

(366)—David Chaum è padre di invenzioni rivoluzionarie nell'ambito della crittografia: teorizza la moneta digitale e il principio delle mix-net. Ma certe proposte recenti prestano il fianco al tecnocontrollo.

22 gennaio 2016—La storia della crittografia è costellata da molti piccoli avanzamenti e poche scoperte rivoluzionarie.

Dopo la prima e fondamentale invenzione del codice cesariano (I sec. a.e.v.), che separa per la prima volta algoritmo e password realizzando così la crittografia moderna, passano una quindicina di secoli abbondanti prima che Giovan Battista Bellaso, Leon Battista Alberti e Blaise de Vigenère facciano una nuova scoperta fondamentale nella scienza della crittografia, sviluppando il metodo della sostituzione polialfabetica.

E, voltando rapidamente le pagine del piccolo libro della Storia della Crittografia, occorre arrivare al ventesimo secolo per vedere un'altra scoperta importante. Sì, perché le novità scoperte nel frattempo, anche cose importantissime come il 3DES, non sono altro che un sofisticato (e possibile solo grazie ai computer) algoritmo di rimescolamento.

Poi dal 1970 al 1980 James H. Ellis, Clifford Cocks, Malcolm J. Williamson (una storia quasi incredibile), Whitfield Diffie e Martin Hellman, Ronald Rivest, Adi Shamir e Leonard Adleman scoprono, ricoprono e biscoprono il metodo crittografico a chiave pubblica (doppia).

Nello stesso periodo un signore chiamato David Chaum, che si era fino ad allora dilettato soltanto con l'invenzione di nuovi algoritmi crittografici, dal 1980 al 1982 realizza da solo ben due invenzioni fondamentali e rivoluzionarie.

Teorizza un metodo per realizzare una moneta digitale ed enuncia il principio delle mix-net che utilizzano anche il metodo di crittografia "a cipolla", alla base dei remailer Cypherpunks e Mixmaster, e che apre la strada che vent'anni dopo ci porterà a Tor."Che uomo, quasi un dio intoccabile!", penseranno adesso alcuni dei 24 increduli lettori.

Sì, ma anche no.

La più recente "invenzione" di David Chaum, il protocollo cMix (qui il paper) e l'applicazione Privategrity forse gli porteranno soldi, ma di sicuro gli hanno attirato le ire di molti suoi colleghi, della comunità open source e dei sostenitori dei diritti digitali.

Dall'altare alle polveri allora? Cosa avrà mai combinato il povero David?Invitando i 24 intrepidi lettori a non lasciarsi intimidire, e dare una scorsa al paper (come sempre la parte iniziale e quella finale sono le più leggibili) per farsi una propria opinione, cerchiamo di riassumere i termini della questione, anzi della nuova "invenzione" di David.

La crittografia, se ben utilizzata dai cittadini digitali, li mette in sicurezza dai criminali che vogliono rubare i soldi del conto corrente telematico o clonare la carta di credito. Se utilizzata con una buona gestione delle chiavi crittografiche e con software verificabili (quindi liberi ed a sorgente aperto) permette anche di sfuggire alle intercettazioni di massa che tanto felici hanno reso i governi di quasi tutti i paesi, non solo quelli a "democrazia limitata" ma anche quelli a "democrazia avanzata".

E, si sa, un governo "infelice" reagisce con forza.

Ed ecco apparire regolamenti e leggi e che richiedono di inserire backdoor nei software crittografici.Ed ecco che, anche senza leggi, arrivano discorsi ambigui di Presidenti una volta detti "progressisti", pressioni dell'FBI, di organizzazioni di polizie europee etc.In questo contesto il buon David se ne esce con un'idea ed una proposta interessante per implementare una comunicazione sicura tra device con bassa potenza di calcolo ed alti volumi di informazioni (smartphone? Ma no!), proponendo appunto il protocollo cMix e l'applicazione Privategrity.

Intendiamoci, la cosa funziona e funziona bene: grazie al precalcolo di alcune informazioni ed all'uso dei più veloci algoritmi a chiave singola rispetto a quelli a chiave doppia, certamente raggiunge gli scopi enunciati.

Peccato che sia facilmente violabile da autorità a livello governativo (e non), e che preveda questa "feature" come caratteristica positiva.

Dove sta l'inghippo? Il sistema è realizzato con un numero limitato di server "certificati" (nove, non le decine di migliaia tra proxy e router di Tor) a cui i vari client si collegano per connettersi in maniera "sicura" utilizzando l'"invenzione" di David. Per far questo devono generare e condividere con ciascun server un diverso segreto (in pratica una password univoca di tipo singolo) destinato ad essere memorizzato su ciascun server per un certo tempo. Questo significa che se un signore con le spalle abbastanza larghe chiede ai gestori di tutti i server **la gentilezza di avere un certo set di 9 password**, il gioco è fatto, e l'utente di Privategrity pure.

Nessuno dei 24 istruiti lettori si aspetterà seriamente che questo venga fatto solo contro i pedoterrosatanisti, ovviamente, ma non è questo il punto.

Un sistema crittografico sicuro non deve dipendere dalla fiducia o dalla buona volontà di una

terza parte: non deve avere segreti condivisi, mai! Se li ha, deve essere messo non nell'arsenale della privacy e della sicurezza informatica ma nel mucchio dei giocattoli e dell'olio di serpente, insieme ai bigliettini cifrati di terza elementare o del metodo Gutmann per la cancellazione sicura dei dischi.Ora, Cassandra è grata, come dovrebbero essere tutti, ad un essere umano che ha fatto a tutti due doni eccezionali.

Questa volta però il nostro David non ci ha fatto un regalo, e per quello che ne pensiamo se lo può tenere e gli auguriamo sinceramente che la sua nuova iniziativa fallisca.

D'altra parte anche altri crittografi contemporanei, ad esempio alcuni di quelli elencati in cima a questa pagina, sono stati sensibilissimi alla cosiddetta "proprietà intellettuale", e sono venuti tranquillamente a patti col Grande Fratello. David è solo un altro della serie.

Probabilmente non è un caso che non sia stato David, inventore del concetto di criptovaluta, a creare la prima criptovaluta di successo, ma ci sia voluto un Satoshi Nakamoto personalità di dubbia esistenza reale, più probabilmente virtuale ed essere etereo della Rete, per realizzare Bitcoin.

Chi fa compromessi perde, almeno in parte, la propria anima e la propria creatività. Comunque, grazie David per quello di buono che ci hai già donato.

Questa volta a Cassandra e soci la tua invenzione non interessa: sarà magari per un'altra volta ed amici come prima.

Originally published at punto-informatico.it.

Scrivere a Cassandra—Twitter—Mastodon
Videorubrica "Quattro chiacchiere con Cassandra"
Lo Slog (Static Blog) di Cassandra
L'archivio di Cassandra: scuola, formazione e pensiero

By Marco A. L. Calamari on June 9, 2022.

Canonical link

Exported from Medium on August 27, 2025.